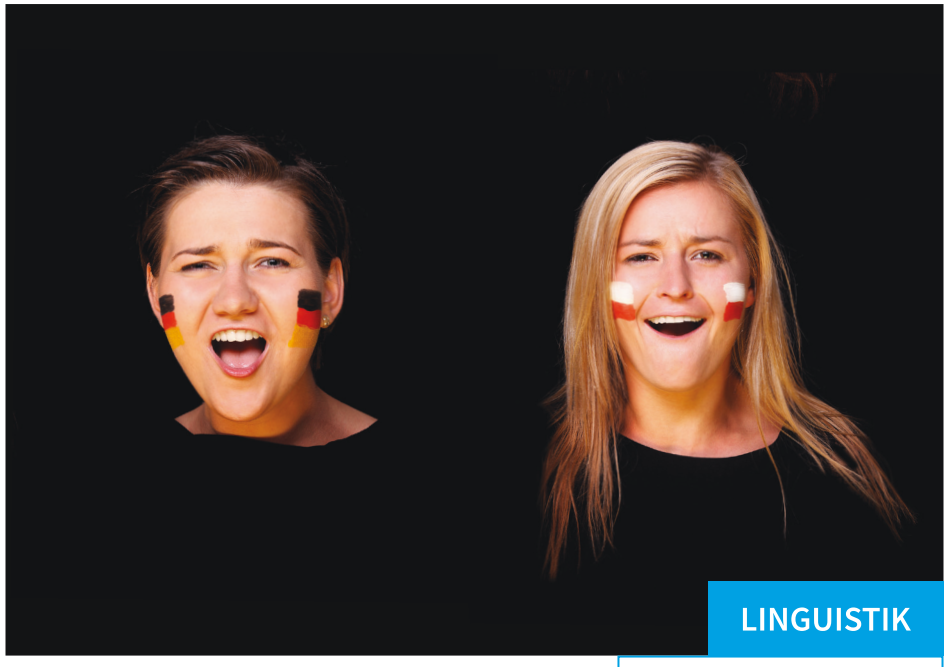
Hg. Dorota Kaczmarek

# Politik – Medien – Sprache

Deutsche und polnische Realien
aus linguistischer Sicht



LINGUISTIK

MEDIENDISKURSE

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

http://dx.doi.org/10.18778/7969-840-0.05

# Kapitel 3

*Philipp Dreesen, Andreas H. Braml*[*]

# Diskurseffekte des NSA-Skandals. Korpusanalyse zu *Verschlüsseln* als kommunikativer Praktik in deutschen Computerzeitschriften 2010–2014

**Zusammenfassung**
Der Beitrag geht der Frage nach, ob und wie sich die massenmediale Berichterstattung über die NSA-Spionageprogramme auf deutsche Computerzeitschriften auswirkt. Anhand der Art und Weise der Behandlung des Themas *Verschlüsselung* wird diskurslinguistisch überprüft, ob es qualitative oder quantitative Veränderungen in den Aussagen gibt, sodass man von *Diskurseffekten* sprechen kann. Das Korpus besteht aus den redaktionellen Beiträgen in COMPUTER BILD und CHIP zwischen 2010 und 2014. Anhand der Berichterstattung über TrueCrypt, De-Mail und PGP kann im Zeitraum der Enthüllungen ein Diskurseffekt nachgewiesen werden, der in der Anleitung zum Verschlüsseln als kommunikative Praktik mündet.

**Schlüsselwörter:** Verschlüsselung, Mail, Überwachung, Datenschutz, NSA

**Abstract**
Discourse Effects of NSA Disclosure. Corpus-based Analysis of ‚Encrypting' as a Communicative Practice in German Computer Magazines 2010 – 2014
This article explores the repercussions – if any – that the broad reception of the 2013 leaks on NSA's surveillance programs in mass media had on German computer magazines. Such *discourse effects* are verified by means of a qualitative and quantitative analysis of the way encryption is handled as a subject, by employing techniques from discourse linguistics. The corpus consists of the editorial content of COMPUTER BILD and CHIP between 2010 and 2014. Looking at the coverage of TrueCrypt, De-Mail and PGP, there can indeed be diagnosed a discourse effect concurrent with the NSA leaks that culminates in instructions on encryption as a communicative practice.

**Keywords:** encrypting, mail, surveillance, data protection, NSA

[*] Dr. Philipp Dreesen (Universität Bremen), Andreas H. Braml (BürgerEnergie Berlin).

## 3.1. Historische und globale Ereignisse – diskursive Bedingungen und Effekte

Von September bis November 2013 fanden die Dreharbeiten zum britisch-angloamerikanischen Spielfilm *The Imitation Game* statt. Das Drama um das Leben von Alan Turing wurde bereits nach seiner Premiere im Sommer 2014 in den USA überaus positiv besprochen. Im Januar 2015 kam der Film in die deutschen Kinos; auch die deutschen Kritiken waren überwiegend gut. Die herausragende Leistung Turings während des Zweiten Weltkriegs bestand in der (auf wichtigen Vorarbeiten des polnischen Mathematikers Marian Rejewski beruhenden) Entzifferung der mittels der Enigma verschlüsselten Nachrichten der Nazis.

Im Juni 2013 berichteten die *Washington Post* und der *Guardian* auf Basis geheimer Dokumente der National Security Agency (NSA) erstmals über die Dimensionen der Ausspähung durch die US-Sicherheitsbehörden. Die sich im Laufe der anschließenden Monate entwickelnde weltweite Berichterstattung wurde unter dem Eindruck der flächendeckenden Überwachung durch das Spionageprogramm PRISM der NSA geführt. Im Zentrum der Berichterstattung und der Diskussion standen dabei insbesondere Fragen nach dem Schutz vor der unbefugten Rezeption privater Daten sowie Fragen nach rechtlicher Begrenzung der Geheimdienstaktivitäten durch internationale Verträge und nationale Gesetze.

Der Erfolg eines Spielfilms, der die Entschlüsselung abgefangener Nachrichten zum Thema hat, und die ungefähr zeitgleichen Enthüllungen über die massenhafte Speicherung abgefangener Nachrichten sind korrelierende, nicht aber zwangsläufig kausal zusammenhängende Ereignisse. Diskursanalytisch betrachtet, handelt es sich um zwei Ereignisse, die durch massenmediale Diskursstrukturen Verbreitung finden und damit überhaupt *thematisierbar* werden (vgl. Dreesen 2015: 303). So wird dem zeitgeschichtlichen Ereignis der Enigma-Entschlüsselung in unserem „kollektiven Gedächtnis" (Assmann 1992) historische Bedeutung zugewiesen. Produziert und aktualisiert wird diese Bedeutung durch die zeitliche Ordnung des Erinnerns und Gedenkens, in diesem Fall 70 Jahre nach Ende des Zweiten Weltkriegs und zum 60. Todestag Turings. Die Berichterstattung zu den globalen Überwachungsaktivitäten der NSA 2013 und der zugeschriebene Status ‚Skandal' beruhen auf der über Jahre bereits zuvor geführten journalistischen Auseinandersetzung um den US-amerikanischen präventiven Generalverdacht.

Diskursanalysen können nicht beantworten, warum ein Film ein Millionenpublikum hat oder warum die Enthüllungen zur NSA weltweit Resonanz erfahren, die dann entgegen der Erwartung vieler recht schnell wieder verebbt (vgl. Morozov 2015: 5). Doch Diskursanalysen – und dies gilt in besonderer Weise für linguistische – ermöglichen den Nachweis über zugrunde liegende Produktionsbedingungen von gegenstandsbezogenen Aussagen:

Die verstreut erscheinenden Aussagen lassen unter der Perspektive einer linguistischen Fragestellung eine Wissens- und Redeordnung erkennen. Jede Aussage setzt das „Aussagengeflecht" (Jung 2006: 38), den Diskurs, fort. In der Konsequenz sind es die Diskurse, „die systematisch die Gegenstände bilden, von denen sie sprechen" (Foucault [1969] 1981: 74).

Unterschiedliche gesellschaftliche Akteure (Institutionen, Personengruppen etc.) haben auf die NSA-Enthüllungen in der massenmedialen Berichterstattung reagiert. So wie der Deutsche Bundestag und das Bundesamt für Sicherheit in der Informationstechnik mit Reden, Maßnahmen und Empfehlungen auf die massenhafte Speicherung und Auswertung von elektronischer Kommunikation reagierten, gilt dies auch für die Anbieter von E-Mail-Diensten sowie Hersteller von Software und Anbieter von Cloud-Diensten (Online-Speicherplätzen). Unter *Diskurseffekt* (vgl. Dreesen 2015: 56) verstehen wir in dieser Untersuchung Aussagen neuer Quantität oder Qualität, die auf die diskursive Berichterstattung über die NSA implizit oder explizit reagieren. Das Aufgreifen des Themas durch die Akteure ist vom Diskurs geprägt. Dabei gehen wir davon aus, dass Akteure in den von ihnen typischerweise produzierten Texten das Thema NSA und Überwachung für gewöhnlich nicht behandeln.

Wir beschränken uns im Folgenden auf die Frage: Wie wird *Verschlüsselung* als kommunikative Praktik vor und nach der massenmedialen Berichterstattung über Snowden und die NSA-Programme in deutschen Computerzeitschriften konstruiert? Die der Analyse zugrunde liegende Hypothese ist, dass Quantität und Qualität der Behandlung von *Verschlüsselung* als diskursive Effekte des sog. NSA-Skandals nachgewiesen werden können; in der Folge wird *Verschlüsselung* als kommunikative Praxis in den Computerzeitschriften erst diskursiv erzeugt.

## 3.2. Diskursanalytische Erfassung des Untersuchungsgegenstands

Die Frage nach dem Effekt der Enthüllungen über die NSA-Programme kann sich auf unterschiedliche Gegenstände, Themen, Akteure, Zeiten, Räume und Medien richten. Mit dem Fokus auf Verschlüsselung blenden wir bewusst die Frage aus, ob und wie über Snowden und die NSA in deutschen Büchern, in Zeitungs- und Magazinartikeln, in Rundfunkbeiträgen und Online-Angeboten berichtet wird. Diskurslinguistische Ansätze erlauben es, einzelne Aussagen nach gegenstandsbezogenen, thematischen, akteursspezifischen, zeitlichen, räumlichen, medialen oder funktionalen Kriterien zu Diskursen zusammenzufassen (vgl. Dreesen 2015: 37, 57). Die einzelnen Aussagen bilden als Aussagengeflecht den zu untersuchenden Diskurs.

*Verschlüsselung* ist ein mathematisch-technischer Vorgang. Während es Wissen gibt, das (massen-)medial aufbereitet und verbreitet wird, gibt es

Wissen, das zwar stark verbreitet ist, aber kaum thematisiert, distribuiert oder öffentlich diskutiert wird (z.B. unser Wissen darüber, wie man sich die Nase putzt). Unser Wissen über Verschlüsselung ist zwar nicht besonders stark verbreitet, es wird aber distribuiert und v.a. in Fachkreisen diskutiert. Während in der professionellen IT-Technik Verschlüsselung unter spezifischen rechtlichen, mathematischen und ökonomischen Aspekten behandelt wird (vgl. Kersten/Klett 2015, Müller 2014, Schwenk 2014), ist vermutlich das massenmedial verbreitete Wissen über Verschlüsselung anders geartet und hängt von der massenmedial vermittelten Gefahr des Datendiebstahls, der Ausspähung und der Möglichkeiten zur Abwehr derselben ab.

Die untersuchten Texte aus den Computerzeitschriften werden als Teil der Wissensordnung über die kommunikative Praktik der Verschlüsselung betrachtet. Das Wissen um Verschlüsselung von E-Mails umfasst eine Reihe von Aspekten: Die Sensibilisierung für die Notwendigkeit von sichernden Vorkehrungen in der Kommunikation, die Risikoabschätzung der elektronischen Datenverschickung, die Fertigkeiten zum Besorgen, Installieren und Anwenden von Software, die gesetzlichen Regelungen, die mathematischen Operationen der Verschlüsselung etc. Nur ein Bruchteil dieses Wissens wird in IT- und Mathematikfachbüchern, in Onlineforen und Computerzeitschriften behandelt und dadurch verbreitet.

Unseren Untersuchungsgegenstand bilden zwei Computerzeitschriften für die Zielgruppe der nicht-professionellen EndanwenderInnen: CHIP und COMPUTER BILD (im Folgenden CB abgekürzt). CHIP gehört zum Burda Media Verlag und erscheint monatlich; CB gehört zum Axel Springer Verlag und erscheint vierzehntäglich. Beide gehören zu den größten themenübergreifenden Computermagazinen in Deutschland. Zielgruppe der Zeitschriften sind private ComputernutzerInnen, die sich über Neuigkeiten, Tests und Anleitungen zu Hard- und Software sowie Technik-Dienstleistungen informieren möchten. Die Redaktionen dieser Magazine bereiten diese Themen für ihre potenziellen LeserInnen auf, indem sie – so unsere Annahme – insbesondere auf gute Verständlichkeit, Entscheidungshilfe und schnelle Anwendbarkeit abzielen.

## 3.3. Verschlüsselung unter kommunikativer und technischer Perspektive

Der Aufwand des technischen Kommunizierens nimmt mit der Zeit ab. Der technische Fortschritt spiegelt sich nicht allein in der verbesserten Reichweite und Qualität der Übertragung wider, sondern auch im Aufwand der NutzerInnen: War es um 1980 trotz vorhandener Leitungen und Apparate – verglichen mit heute – aufwändig, jemanden fernmündlich zu kontaktieren (Nummer

heraussuchen, Freizeichen abwarten, wählen, auf Entgegennahme des Anrufes warten), ist der Aufwand über die Zeit kontinuierlich gesunken: Durch eingespeicherte und erkennbare Rufnummern, durch Angebote wie SMS sinkt der Aufwand, jemanden zu erreichen; zugleich sind viele NutzerInnen durch Skype, Facebook, Twitter, WhatsApp im Internet/WWW permanent (potenziell) miteinander in Kontakt und ihre Tätigkeiten synchronisiert. Damit stellen sich Fragen, wie und ob ich jemanden erreiche bzw. erreichen kann, in dieser Weise nicht mehr. Der technische Fortschritt hat dabei nicht zu einer Ablösung von Kommunikationstechniken gesorgt, eher sind zu etablierten Techniken neue Optionen getreten, die sich z. T. als Standards für bestimmte Gesprächsabsichten und -inhalte durchgesetzt haben. Kiesendahl (2011: 318) schreibt zur Wahl zwischen E-Mail und face-to-face-Kommunikation, die Anpassung des Handlungszwecks und die Wahl der (verbalen) Zeichen „an die mediale Realisierung erzeugt erst ein auf allen Ebenen normenadäquates Kommunikat". Über die mediale Realisierung i.e.S. hinaus hat sich die Medienkompetenz im Umgang mit den neuen Risiken hinsichtlich der Wahrung von vertraulichen Nachrichten in der elektronischen Datenübertragung noch nicht entwickelt. Kompetenter Umgang mit E-Mails meint nicht nur sicheres Erstellen, sondern umfasst auch das Erkennen vertrauenswürdiger Inhalte, sichere Kommunikationsverfahren sowie nachvollziehbare Speicherverfahren und -orte.

Sprachwissenschaftlich betrachtet, kann die Verständigung mit E-Mails als Textnachrichten und damit als „zerdehnte Sprechsituation" (Ehlich 1984) bezeichnet werden. In der überwiegend asynchronen Kommunikationssituation des E-Mail-Verkehrs wird der Kanal – außer bei Störungen – so gut wie nicht beachtet. Die Notwendigkeit von Verschlüsselung ist darin begründet, dass E-Mail-Kommunikation das Internet als Transportweg nutzt, wobei Datenpakete vielfach Staats- und Konzerngrenzen passieren. Absender und Empfänger haben keine Kontrolle darüber, was mit den Metadaten sowie den Inhalten der E-Mails während der Übertragung geschieht.

Mit Goffman (1981: 131–135) können wir im kommunikativen Austausch drei Typen von Rezipierenden unterscheiden: (1) Adressierte zuhörende Akteure, d.h., Rezipienten sind intendierte Empfänger der Nachricht; (2) zufällig mithörende Akteure („adventitious participants"), d.h., beispielsweise bekommt eine vorbeigehende Passantin einige Gesprächsinhalte mit, was weder intendiert noch vom Sender autorisiert wurde; (3) gezielt mithörende Akteure, d.h., es wird aktiv der Versuch unternommen, die nicht an Dritte gerichtete Nachricht rezipieren zu können. In der nachrichtendienstlichen Tätigkeit des Abfangens elektronischer Nachrichten von fremden Akteuren handelt es sich eindeutig um Typ 3.

*Verschlüsseln* ist eine kommunikative Praktik. Unter kommunikativen Praktiken verstehen wir nach Fiehler (2004: 15–17) routinisierte Handlungen, die

nach sozialen Regeln zur Lösung von kommunikativen Herausforderungen eingesetzt werden. Dabei bedingen Regeln und Praktik einander. Praktiken sind zwar intentional, nicht aber notwendigerweise bewusst. Kommunikative Praktiken sind nicht grundsätzlich an eine Realisierung (Mündlichkeit, Schriftlichkeit) gebunden oder gattungs-, text- und medienspezifisch. Unseres Erachtens hängt der Status ‚Praktik' nicht von der Verbreitung derselben ab; entscheidend ist die Abstraktion von der konkreten Handlung (z.B. Bedienen eines Verschlüsselungsprogramms oder Anwendung einer Geheimschrift). *Verschlüsselung* ist demnach nicht allein eine bewusste Handlung zur Erreichung eines Ziels, sondern eine im Sozialen liegende Praktik in Übereinstimmung mit Regeln und Normen.

In der Fachliteratur zur IT-Sicherheit[1] wird Verschlüsselung als eine Maßnahme in einer Kette von Vorüberlegungen, Bedingungen und Handlungen zur Sicherung eingebettet (vgl. z.B. Kersten/Klett 2015: 1–22, Müller 2014: 13, 146–160). Verschlüsselung, so die fachliche Sicht, ist erst dann sinnvoll, wenn die „Vertrauenswürdigkeit" (vgl. dazu grundlegend Schäfer 2013: 72–89) der Kommunizierenden sichergestellt ist und im Idealfall in der IT-Kommunikation ein Vertrauenszirkel entsteht (vgl. Müller 2014: 102–103). Verschlüsselung umfasst demnach sowohl das grundlegende Verständnis um die Notwendigkeit von sichernden Vorkehrungen als auch die Risikoabschätzung der elektronischen Datenverschickung sowie das hierfür notwendige technische Verständnis. Ziel der Verschlüsselung ist – wie aller IT-Sicherheitsmaßnahmen – die Aufrechterhaltung der Datenintegrität, hier der verschickten E-Mail. Es können prinzipiell fast alle Elemente der E-Mail (Empfänger, Betreff, Nachrichtentext, Anhänge) verschlüsselt werden.

Um zu verhindern, dass die kooperative Absicht des Senders an den Empfänger durch Dritte gestört wird, kann mit Verschlüsselungstechnik zumindest Zweierlei verhindert werden (nach Kersten/Klett 2015: 245): Erstens wird die unbefugte Kenntnisnahme von Daten unterbunden, also das Abhören im engeren Sinne. Zweitens wird die Manipulation von Daten auf dem Transfer verhindert, beispielsweise unterstützt durch die Prüfsumme der verschickten Daten (vgl. Kersten/Klett 2015: 224). Das Verhindern des Abhörens und der Manipulation der Daten auf dem Transportweg schützt indes nicht vor unerwünschten Vorgängen/Aktionen beim Sender und Empfänger. Eine verschlüsselte Nachricht ist ab dem Moment nicht mehr vor Dritten sicher, in dem die Nachricht, etwa auf dem heimischen Rechner, entschlüsselt ist und in der Folge unverschlüsselt abgespeichert wird (etwa auf der eigenen Festplatte oder in der Cloud).

Um Verschlüsselung für kommunikativen Austausch nutzen zu können, ist ein Schlüssel auf der Basis eines umkehrbaren Algorithmus notwendig (vgl. Kersten/Klett 2015: 213): Wäre er nicht umkehrbar, könnte man die Nachricht

[1] Zum Verschlüsseln im nicht technischen Sinne vgl. Pappert/Schröter/Fix 2008.

zwar ver-, aber nicht mehr entschlüsseln. Die Stärke der Verschlüsselung hängt von der mathematischen Qualität des Algorithmus und von der Länge des Schlüssels ab (vgl. Kersten/Klett 2015). Der Schlüssel wird überwiegend über eine Krypto-Software nach Zufallsprinzip erzeugt. Ver- und Entschlüsselung kann symmetrisch oder asymmetrisch erfolgen: Beim symmetrischen Verfahren wird für das Verschlüsseln und Entschlüsseln der gleiche Schlüssel verwendet. Beim sichereren asymmetrischen Verfahren besitzt jeder Kommunikationspartner zwei unterschiedliche Schlüssel (ein Schlüsselpaar),

> einen zum Verschlüsseln, einen zweiten zum Entschlüsseln von Daten. Der zum Verschlüsseln vorgesehene Schlüssel wird als *öffentlicher Schlüssel* (*Public Key*) bezeichnet und kann mit dem Namen seines Besitzers
> – in ein öffentlich zugängliches Verzeichnis (*Public Key Directory*) eingestellt werden oder
> – an potenzielle Kommunikationspartner auf anderem Wege (z. B. per E-Mail) gesandt werden.
>
> Mit diesem Public Key kann *jeder* Daten verschlüsseln – aber nur der Besitzer des dazu passenden zweiten Schlüssels ist in der Lage, die Daten zu entschlüsseln. Der zweite Schlüssel wird *geheimer Schlüssel* (*Private Key*) genannt und ist von seinem Besitzer sicher aufzubewahren (Kersten/Klett 2015: 219; Herv. i. Orig.).

Abhängig von der Stärke des Schlüssels ist es nahezu unmöglich, aus dem öffentlichen Schlüssel den dazugehörenden privaten (also geheimen) Schlüssel zu berechnen (vgl. Kersten/Klett 2015: 220). In der IT-Sicherheit herrscht Einigkeit darüber, dass die derzeit sicherste Verschlüsselung die sog. Ende-zu-Ende-Verschlüsselung darstellt. Bei ihr werden die versandten Nachrichten nicht auf dem Transportweg entschlüsselt, sondern bleiben bis zur Entschlüsselung durch den Adressaten für Dritte unzugänglich. Dies unterscheidet die Ende-zu-Ende-Verschlüsselung von Diensten, die zwar eine Verschlüsselung auf dem Transportweg ohne Zutun der Nutzer zusichern; eine Überprüfung, ob und wie weit diese Zusicherung eingehalten wird, ist letztlich jedoch nicht möglich.

## 3.4. Korpora und Analyse

### 3.4.1. Korpora

Die Korpora sind mittels der Datenbank *Factiva* zusammengestellt (https://global.factiva.com). Die Recherchefunktion ermöglicht die Volltextsuche. Die Korpora bestehen aus redaktionellen Inhalten (Artikeln, Beschreibungen, Ankündigungen, Hinweisen, Tests) der Printausgaben der Computerzeitschriften COMPUTER BILD (CB) und CHIP. Die entsprechenden Websites der Magazine wurden nicht berücksichtigt.

Das erste Korpus (Schlüssel-Korpus) besteht aus allen Artikeln, die zwischen dem 01.01.2010 und dem 31.12.2014 in den beiden Zeitschriften erschienen sind und die präfigierten Derivationen *verschlüssel* oder *entschlüssel* enthalten, z.B. das Verb *verschlüsseln*, das Partizip *verschlüsselnd*, das Substantiv *Entschlüsselung*. Pre-Tests mit den Ausdrücken[2] *enigmail*, *truecrypt*, *gnu*, *pgp*, *gpg*, *de-mail*, *ssl*, *tls*, *aes*, *kerberos*, *krypto* waren dahingehend ergebnislos, dass alle Artikel mit dem Gegenstand *Verschlüsselung* auch *verschlüssel* oder *entschlüssel* enthalten. D.h., beispielsweise enthalten alle Artikel zum Verschlüsselungsprogramm TrueCrypt auch einen deutschen Ausdruck mit dem Morphem *{schlüssel}*. Die Suche nach dem Basismorphem *{schlüssel}* erwies sich als nicht weiterführend, da die häufige Thematisierung Lizenzierung unterliegender Software das Wort *Schlüssel* und das Kompositum *Lizenzschlüssel* aufweist. Das zweite Korpus (De-Mail-Korpus) besteht aus den Zeitschriftenartikeln des gleichen Zeitraums, die den Ausdruck *de-mail* enthalten. Das dritte Korpus (TrueCrypt-Korpus) bilden Artikel mit dem Ausdruck *truecrypt*, einem bekannten Verschlüsselungsprogramm. Das vierte Korpus besteht aus Artikeln zum Verschlüsselungsprogramm PGP (PGP-Korpus).

Die Analyse beschränkt sich auf subsyntaktische Einheiten. Wie bereits anhand der Korpuszusammenstellung ersichtlich, erfolgen Zugriff auf das Thema und die Filterung einzelner Aspekte über Schlüsselbegriffe.

### 3.4.2. Analyseergebnisse

Über den Zeitraum von fünf Jahren zeigt sich ein deutlicher Anstieg der Verwendung von *verschlüssel* oder *entschlüssel* in redaktionellen Beiträgen von CB und CHIP (vgl. Tab. 3.1).

Tabelle 3.1: Verteilung von Beiträgen mit verschlüssel/entschlüssel im Schlüsselkorpus

| Jahr | CB | CHIP | Gesamtbeitragsanzahl |
|---|---|---|---|
| 2010 | 97 | 50 | 147 |
| 2011 | 79 | 88 | 167 |
| 2012 | 85 | 71 | 156 |
| 2013 | 76 | 88 | 164 |
| 2014 | 107 | 95 | 202 |
| **2010–2014** | **444** | **392** | **836** |

[2] Die Liste enthält aus onomasiologischer Perspektive die Ausdrücke, die dem Gegenstand *Verschlüsseln* als technisches Verfahren im Rahmen der Computerzeitschriften zufallen.

Die Tabellenzahlen sind nicht bereinigt, d.h., es sind auch Artikel enthalten, die sich z. B. mit Verschlüsselung von TV-Programmen und Router-Einstellungen befassen. Die quantitative Verteilung gibt also noch keinen Aufschluss über einen diskursiven Effekt der NSA-Enthüllungen auf die Thematisierung von Verschlüsselung für Privatanwender, wenngleich die Spitzenwerte von 167 und 205 Beiträgen 2013/2014 mit der Berichterstattung über Edward Snowden und der NSA-Affäre zusammenfallen.

Differenziert nach Zeitschriften zeigt sich, dass im Jahr 2010 Artikel mit *verschlüssel* oder *entschlüssel* in CB ungefähr doppelt so häufig auftauchen wie in CHIP. In den Folgejahren gleichen sich die Zahlen in etwa an: Zu Beginn der massenmedialen Berichterstattung ist kaum ein Unterschied zwischen CB und CHIP hinsichtlich der Artikelanzahl mit *verschlüssel*/*entschlüssel* auszumachen. Gemessen an den vorliegenden Beitragszahlen pro Jahr ist in CB zwischen 2010 (102 Beiträge) und 2014 (110 Beiträge) kein diskursiver Effekt des NSA-Skandals nachzuweisen.

Da die reine Häufigkeit keinen Aufschluss über den diskursiven Effekt gibt, haben wir nach der thematischen Berichterstattung zur Datenverschlüsselung gesucht. Das Korpus zeigt von seinen ersten Beiträgen vom Januar 2010 bis zum Juni 2013 folgendes Bild: Wie erwartet behandeln CHIP und CB das Thema Sicherheit durch Verschlüsselung von Daten vor allem stark endanwenderbezogen, hier vor allem durch die Empfehlung der kostenlosen Verschlüsselungssoftware TrueCrypt (vgl. Tab. 3.2). Die Verschlüsselung von Daten auf Festplatten, auf USB-Sticks und in Webspace/Clouds mit TrueCrypt wird hinsichtlich Benutzerfreundlichkeit, Kompatibilität und des Verschlüsslungs-Algorithmus getestet (vgl. z. B. „Schlüsselfertig“ vom 9. April 2011 CB). Allerdings ist die Verschlüsselung von E-Mails mit TrueCrypt nicht möglich, sodass folglich dieser Aspekt in den Artikeln nicht behandelt wird. Es ist kein diskursiver Effekt des NSA-Skandals nachzuweisen; irrierend ist der hohe Wert in CHIP 2011, also vor den NSA-Enthüllungen.

Tabelle 3.2: Verteilung von Beiträgen im TrueCrypt-Korpus

| Jahr | CB | CHIP | Gesamtbeitragsanzahl |
|---|---|---|---|
| 2010 | 2 | 4 | 6 |
| 2011 | 3 | 11 | 14 |
| 2012 | 1 | 4 | 5 |
| 2013 | 3 | 4 | 7 |
| 2014 | 3 | 4 | 7 |
| **2010–2014** | **12** | **27** | **39** |

Parallel zur Darstellung der Verschlüsselungssoftware TrueCrypt wird über die Einführung von De-Mail in Deutschland berichtet. Der Testbetrieb dieser vom Anbieter für verschlüsselt erklärten Art der E-Mail-Kommunikation läuft im Jahr 2009 an. Vor dem Hintergrund des bereits bestehenden Dienstes E-Post der Deutschen Post AG werden die Vor- und Nachteile von De-Mail in CB und in CHIP erörtert.

Tabelle 3.3: Verteilung von Beiträgen im De-Mail-Korpus

| Jahr | CB | CHIP | Gesamtbeitragsanzahl |
|---|---|---|---|
| 2010 | 5 | 0 | 5 |
| 2011 | 2 | 3 | 5 |
| 2012 | 2 | 4 | 6 |
| 2013 | 0 | 4 | 4 |
| 2014 | 1 | 1 | 2 |
| **2010–2014** | **10** | **12** | **22** |

Tabelle 3.3 stellt dar, dass die Erwähnung von *de-mail* (datenbereinigt) in den Gesamtzahlen relativ konstant über den Zeitraum 2010 bis 2013 bleibt. Große Unterschiede zeigen sich in der Berichterstattung zu Beginn der Einführung von De-Mail (2010) und im Jahr der Enthüllungen über die NSA (2013): Zu Beginn von De-Mail ist CHIP zurückhaltend, zu Beginn des NSA-Skandals wird CB zurückhaltend. Geht man diesem Befund zur Berichterstattung über De-Mail genauer nach, so ergibt sich folgendes Bild: In den zwölf Artikeln in CHIP mit dem Ausdruck *de-mail* geht es um mögliche Anbieter, Sicherheit, Rechte und Pflichten von Anbietern und Nutzern. In fünf der zwölf Artikel kommt *verschlüssel* und *entschlüssel* vor. Ein weiterer Artikel behandelt das Thema ‚Sicherheit', ohne dass *verschlüssel* und *entschlüssel* vorkommt (vgl. Tab. 3.4; Doppelzählungen sind möglich).

Die Zunahme der Relevanz von E-Mail-Verschlüsselung kann anhand der Berichterstattung über De-Mail nachgewiesen werden. Die Textsorten zum Gegenstand wandeln sich, der Fokus verschiebt sich und Stimmen in den Texten wechseln. Die fünf Artikel von 2011 bis November 2012 sind kurze Nachrichtentexte, die von der bevorstehenden Einführung von De-Mail und Streit zwischen den Anbietern berichten. Anschließend werden die Artikel kritischer. Es zeigt sich, dass Sicherheit ein durchgehendes Thema der Berichterstattung über De-Mail ist. Die Filterung nach *{sicher}* zeigt einen Anstieg des Themas im Jahr 2013. Um genauer zu bestimmen, wie *{sicher}* morpho-syntaktisch verwendet wird und welche Bedeutung transportiert wird, ist zunächst die Fokussierung unterteilt

Tabelle 3.4: CHIP-Beiträge, unterteilt nach Suchausdrücken, im De-Mail-Korpus

| **Jahr** | **Gesamtbeitrags-anzahl mit *de-mail*** | **Beiträge mit *verschlüs-sel, entschlüssel*** | **Beiträge mit {*sicher*}** | **Beiträge mit *rechtssicher*** |
|---|---|---|---|---|
| 2010 | 0 | 0 | 0 | 0 |
| 2011 | 3 | 1 | 2 | 2 |
| 2012 | 4 | 1 | 2 | 1 |
| 2013 | 4 | 3 | 4 | 1 |
| 2014 | 1 | 0 | 1 | 1 |
| **2010–2014** | **12** | **5** | **9** | **5** |

worden. Die Filterung nach *rechtssicher* ergibt, dass Sicherheit v. a. unter dem Aspekt der rechtsverbindlichen Kommunikation behandelt wird, also insbesondere der Frage, ob eine Nachricht als zugestellt anerkannt wird. Die Artikel ab November 2012 behandeln Sicherheit unter Datenschutzgesichtspunkten. Wie man erkennt, wird offenbar auch Verschlüsselung bzw. Entschlüsselung (*verschlüssel*/*entschlüssel*) im Jahr 2013 in der Berichterstattung zentral.

In den (datenbereinigt) zehn Artikeln in CB mit dem Ausdruck *de-mail* geht es ebenfalls um mögliche Anbieter, Sicherheit, Rechte und Pflichten von Anbietern und Nutzern (vgl. Tab. 3.5). In fünf der zwölf Artikel kommt *verschlüssel*/*entschlüssel* vor. Ein weiterer Artikel behandelt das Thema Sicherheit, ohne dass der Ausdruck *sicher* vorkommt.

Tabelle 3.5: CB-Beiträge, unterteilt nach Suchausdrücken im De-Mail-Korpus

| **Jahr** | **Gesamtbeitrags-anzahl mit *de-mail*** | **Beiträge mit *verschlüs-sel, entschlüssel*** | **Beiträge mit *{sicher}*** | **Beiträge mit *rechtssicher*** |
|---|---|---|---|---|
| 2010 | 5 | 3 | 5 | 3 |
| 2011 | 2 | 0 | 2 | 1 |
| 2012 | 2 | 1 | 1 | 1 |
| 2013 | 0 | 0 | 0 | 0 |
| 2014 | 1 | 1 | 1 | 0 |
| **2010–2014** | **10** | **5** | **9** | **5** |

Die Behandlung des Aspekts der Verschlüsselung nimmt nach den Berichten zur Einführung von De-Mail (2010) ab. Deutlich erkennbar ist auch, dass das Thema Sicherheit eher mit der Frage der Rechtssicherheit (siehe

oben) verknüpft ist. Kontrastierend zeigt sich, dass die Berichterstattung zu De-Mail in CHIP zwar wesentlich später beginnt, in Hinblick auf die Frage nach Sicherheit (und Verschlüsselung) aber kritischer ist.

Eine derzeit sichere (auch von EndanwenderInnen) beherrschbare Verschlüsselungstechnik ist das oben (vgl. Kap. 3.4.1) erwähnte Verfahren PGP (Pretty Good Privacy), insbesondere dessen freie und kostenlose Implementierung GPG (GNU Privacy Guard). Das von uns erstelle PGP-Korpus enthält alle Artikel mit dem Ausdruck *pgp* oder *gpg*. Da diese Graphemreihenfolge im Deutschen nicht vorkommt, referieren alle Artikel auf die genannte Verschlüsselungstechnik.

Tabelle 3.6: Verteilung von pgp/gpg im PGP-Korpus

| Jahr | CB | CHIP | Gesamtbeitragsanzahl |
|---|---|---|---|
| 2010 | 0 | 0 | 0 |
| 2011 | 0 | 0 | 0 |
| 2012 | 0 | 1 | 1 |
| 2013 | 3 | 5 | 8 |
| 2014 | 0 | 5 | 5 |
| **2010–2014** | **3** | **11** | **14** |

Deutlich wird (vgl. Tab. 3.6), dass CB das Thema erst im Jahr des NSA-Skandals aufgreift, was auch explizit in zwei der drei Beiträge benannt wird. Der dritte Beitrag erwähnt den PGP-Erfinder, handelt aber nicht von der Technik selbst. Betrachtet man die drei Artikel in CB näher, stellt man fest, dass die Redaktion die Verschlüsselungstechnik ablehnt, sogar vor ihr warnt: „Vergessen Sie PGP &Co!“ („Angie, DAMIT wäre es nicht passiert!“ vom 30. November 2013) sowie:

> Eine wirksame Schutzmethode ist die Verschlüsselung der elektronischen Post. Übliche Techniken wie PGP (siehe Kasten rechts) sind aber nur für Profis empfehlenswert, da sie in der Regel teuer und kompliziert sind.“ („Schutz vor der Spionage. Damit stoppen sie Obamas Internet-Spione“ vom 13. Juli 2013)

In diesem ausführlichen Artikel wird ein recht hoher Aufwand betrieben, um die LeserInnen von PGP abzuhalten. Die Redakteure setzen sich mit der von Experten als derzeit sichersten eingeschätzten sichersten Verschlüsselungstechnik auseinander, raten aber den LeserInnen von der etablierten Technik ab und empfehlen eine redaktionelle Eigenentwicklung, bei der Nachrichten als mit Passwort geschütztes Zip-Archiv an eine

gewöhnliche E-Mail angehängt verschickt werden sollen. Das Problem der sicheren Passwortübermittlung, also des Schlüssels für die Entschlüsselung des Archivs, wird dadurch gelöst, dass es aus dem Online-Übertragungsweg ausgeklammert wird: Das Passwort soll, so die Empfehlung, per Telefon oder persönlich übermittelt werden. *Verschlüsselung* wird also als eine kommunikative Praktik konstruiert, die a) nicht auf bestehende Techniken zurückgreifen kann; b) individuelle Lösungen für EndanwenderInnen erfordert; c) sich letztlich nicht sicher online umsetzen lässt.

Wesentlich differenzierter fällt die Auseinandersetzung mit PGP/GPG in CHIP aus. Die Auseinandersetzungen mit GPG sind unmittelbare Effekte auf die NSA-Enthüllungen. So heißt es explizit:

> Zum einen sollten User nur einen deutschen E-Mail-Provider nutzen. Dieser kann nicht ohne Weiteres von den NSA-Schnüfflern ausgelesen werden. („So schützen Sie sich" vom 1. August 2013).

Für die Deutung der Artikel als Reaktion auf die NSA spricht auch, dass die Hefte Anleitungen zur Installation und Nutzung von PGP-Software mit expliziter Nennung der NSA-Überwachung als Anlass enthalten (vgl. „Wege aus der NSA-Überwachung" vom 1. März 2014, vgl. Heft vom 1. Juli 2014 und 1. Oktober 2014). Die Berichterstattung wird komplexer und kommt zu differenzierten Urteilen über die Leistungsfähigkeit von PGP (vgl. „Verschlüsselung für Thunderbird einrichten" vom 1. September 2013).

## 3.5. Fazit und Ausblick

Die spezifische diskursive Ordnung von Computerzeitschriften scheint für die Behandlung des Themas Datenschutz qua Verschlüsselung eher ungeeignet zu sein. Zwar können Zeitschriften auf aktuelle Ereignisse in der Regel recht schnell reagieren, doch offenbar prägen die redaktionellen Strukturen die Verarbeitung und Aufarbeitung von Themen in spezifischer Weise. Die Zeitschriften behandeln das Thema nicht politisch, sondern ausschließlich technisch auf einem offenbar für die EndanwenderInnen angenommenen Niveau. Insofern ist der Rückschluss von der Nennung politischer Institutionen wie *NSA*, *Geheimdienste*, *Kanzlerin* auf einen thematisch-funktionalen politischen Inhalt nicht möglich. Demgemäß geht es bei der thematisierten Verschlüsselung z.B. nicht um den Umstand, dass die NSA verschlüsselte im Gegensatz zu unverschlüsselten Nachrichten dauerhaft speichert (vgl. Bendrath 2014: 25), sondern allein darum, welche technischen Möglichkeiten für die Heimanwendung sinnvoll sind.

Die diskursive redaktionelle Ordnung zeigt sich zudem darin, dass sich die technisch naheliegende und sinnvolle Verknüpfung der Anwendung des

in den Zeitschriften vielbeworbenen Verschlüsselungsprogramms TrueCrypt mit De-Mail in den drei Korpora (Schlüssel-, TrueCrypt-, De-Mail-Korpus) nicht findet. Dies gibt Aufschlüsse über die Konzeptualisierung von *Verschlüsselung* durch CHIP und CB: Verschlüsselung wird offenbar nicht als eine technische Lösung eines manifesten Problems in der Online-Nachrichtenübermittlung angesehen, sondern das Problem wird der Ordnung der Zeitschriftenrubriken gemäß behandelt: Berichterstattung über technische Neuerungen sind von Software- und Sicherheits-Empfehlungen strikt getrennt; die Verschlüsselung heimischer Daten gehört einer anderen Rubrik im Heft an als der sichere E-Mail-Verkehr. Erst der NSA-Skandal führt zur Auflösung derartiger diskursiver Trennungen: Die Problematisierung der nicht gewährleisteten Ende-zu-Ende-Verschlüsselung bei De-Mail kann mittels PGP-Verfahren gelöst werden, berichtet CHIP im August 2013 (vgl. „Das große FAQ-Special zur De-mail" vom 1. August 2013). In den Beiträgen in Reaktion auf die NSA-Berichterstattung wird Verschlüsselung von E-Mails als kommunikative Praxis zum ersten Mal sichtbar – dies ist ein diskursiver Effekt.

Die Enigma-Verschlüsslung wurde insbesondere aufgrund der Wiederholung von einleitenden, textklassifizierenden und adressatenbezogenen Wörtern und Phrasen entschlüsselt. Nicht die Verschlüsselungstechnik selbst war in diesem Fall die Achillesverse der sicheren Datenübertragung, sondern die Anwender der Verschlüsselungstechnik, in diesem Fall das die Nachrichtentexte produzierende Oberkommando der Wehrmacht. Jede Verschlüsselung ist letztlich nur so gut, wie die AnwenderInnen das dahinterstehende Prinzip verinnerlicht haben – und das heißt, es als kommunikative Praktik erlernt haben.

## Literatur

**Quellen**

CHIP. Deutsches Technikmagazin, Ausgaben vom 1. Januar 2010 bis 1. Dezember 2014.

COMPUTER BILD. Deutsche Computerzeitschrift, Ausgaben vom 4. Januar 2010 bis 13. Dezember 2014.

**Forschungsliteratur**

Assmann, Jan (1992): *Das kulturelle Gedächtnis. Schrift, Erinnerung und politische Identität in frühen Hochkulturen.* München.

Bendrath, Ralf (2014): Überwachungstechnologien. In: *Aus Politik und Zeitgeschichte* 18–19, S. 20–25.

Dreesen, Philipp (2015): *Diskursgrenzen. Typen und Funktionen sprachlichen Widerstands auf den Straßen der DDR*. (Diskursmuster – Discourse Patterns, 8). Berlin, Boston.

Ehlich, Konrad (1984) Zum Textbegriff. In: Rothkegel, Annely/Sandig, Barbara (Hg.): *Text – Textsorten – Semantik.* Hamburg, S. 9–25.

Fiehler, Reinhard/Barden, Birgit/Elstermann, Mechthild/Kraft, Barbara (2004): *Eigenschaften gesprochener Sprache*. Tübingen.

Foucault, Michel [1969] (1981): *Archäologie des Wissens*. Frankfurt a.M.

Goffman, Ervin (1981): *Forms of Talk*. Pennsylvania.

Jung, Matthias (2006): Linguistische Diskurshistorische Analyse – eine linguistische Perspektive. In: Reiner, Keller/Andreas, Hirseland/Werner, Schneider/Willy, Viehöver (Hrsg.), *Handbuch sozialwissenschaftliche Diskursanalyse*. Bd. 1: Theorien und Methoden. Wiesbaden (2. aktualisierte u. erweiterte Aufl.), S. 31–53.

Kersten, Heinrich/Klett, Gerhard (2015): *Der IT Security Manager. Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden*. 4. Aufl. Wiesbaden.

Kiesendahl, Jana (2011): *Status und Kommunikation. Ein Vergleich von Sprechhandlungen in universitären E-Mails und Sprechstundengesprächen*. (Philologische Studien und Quellen, 227). Berlin.

Morozov, Evgeny (2015): „Ich habe doch nichts zu verbergen". In: *Aus Politik und Zeitgeschichte* 11–12, S. 3–7.

Müller, Klaus-Rainer (2014): *IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices*. 5., neu bearb. u. erg. Aufl. 2014. Wiesbaden.

Pappert, Steffen/Schröter, Melani/Fix, Ulla (2008): *Verschlüsseln, Verbergen, Verdecken in öffentlicher und institutioneller Kommunikation*. (Philologische Studien und Quellen, Heft 211). Berlin.

Schäfer, Pavla (2013): *Das Potenzial der Vertrauensförderung. Sprachwissenschaftliche Explikation anhand von Texten der Brücke-Most-Stiftung*. (Philologische Studien und Quellen, 243). Berlin.

Schwenk, Jörg (2014): *Sicherheit und Kryptographie im Internet. Theorie und Praxis.* 4., überarb. u. erw. Aufl. 2014. Wiesbaden.

Dr. Philipp Dreesen
Universität Bremen
Deutsche Sprachwissenschaft/Interdisziplinäre Linguistik
E-Mail: philipp.dreesen@uni-bremen.de

Andreas H. Braml
BürgerEnergie Berlin eG
Netzwerkadministration
E-Mail: a.braml@buerger-energie-berlin.de

LINGUISTIK | MEDIENDISKURSE

Den im Band präsentierten Beiträgen liegt sowohl theoretisch als auch empirisch eine medienlinguistische Perspektive in der Betrachtung gegenwärtiger gesellschaftspolitischer Ereignisse in Deutschland und Polen, die in letzter Zeit viele kontroverse Debatten hervorgerufen haben, zugrunde. Die gezeigten unterschiedlichen Möglichkeiten der Vernetzung linguistischer und medienorientierter Forschungen resultieren deshalb aus der Überzeugung, dass die Medien die Welt der Politik auf ihre Art interpretieren, und zwar mit verschiedenen sprachlichen und visuellen Mitteln.

Nicht nur in der theoretisch-empirischen Reflexion über die neusten Verschränkungen der Politik, Medien und Sprache sind aber die Vorteile dieser Arbeit zu sehen, sie betreffen auch text- und diskursanalytische Vorschläge der Interpretation solcher Vernetzungen, die besonders für Studierende, Doktoranden der linguistischen und journalistischen Studienrichtungen sowie andere Interessierte inspirierend sein können.

WYDAWNICTWO UNIWERSYTETU ŁÓDZKIEGO

ul. Williama Lindleya 8
90-131 Łódź

tel.: 42 66 55 863
fax: 42 66 55 862
e-mail: ksiegarnia@uni.lodz.pl

ISBN 978-83-7969-840-0